BSA Principles for Securing the IoT

As trusted leaders in the global software industry, BSA members are at the forefront of Internet of Things (IoT) innovation, including advancements in IoT security. BSA endorses the following principles for building trust in the IoT that embody a responsible, risk-based approach to government IoT security policy.

1. **Account for the IoT ecosystem's diversity and complexity.** Holistically consider the complexity and diversity of the IoT ecosystem, recognizing the unique role each part of the system plays and how those parts interact, and design policies that are technology-neutral and flexible to accommodate such complexity.

2. **Define key concepts and requirements clearly.** Clearly define key concepts and requirements related to IoT security, such as "IoT" and "IoT device."

3. **Secure the whole IoT ecosystem, not just devices.** Drive a risk-based approach to trust and safety by considering software, firmware, and hardware deployed throughout IoT technologies, and avoiding device-centric policies that disrupt sophisticated network-based security measures.

4. **Distinguish between consumer IoT and industrial IoT (IIoT).** Address the different risks posed by consumer IoT and IIoT technologies, rather than pursuing one-size-fits-all approaches. Policies for consumer devices may need to prioritize building security into devices, while industrial users may need more flexibility to tailor security measures to their unique, complex operating environments.

5. **Build on industry best practices.** Be informed by the expertise of industry leaders and incorporate widely accepted, risk-based IoT security best practices developed by industry to elevate the security of the entire IoT market.

6. **Incentivize security throughout the IoT life cycle.** Incentivize businesses to voluntarily establish coordinated vulnerability disclosure processes and end-of-life policies to promote security throughout the IoT life cycle.

7. **Embrace multi-stakeholder processes.** Leverage multistakeholder processes to collaborate with industry and develop best practices for IoT security based on existing, consensus-based guidelines.

8. **Seek national and international policy harmonization.** Align IoT security policies, to the greatest extent possible, with other similar efforts underway around the world.

9. **Support the development and use of internationally recognized IoT standards.** Link IoT security policies to global, voluntary, and consensus-based standards wherever they exist, and support the development of new international recognized IoT security standards.

10. **Establish baseline security requirements as necessary and appropriate.** Align core security capabilities, where necessary, with widely accepted international standards, which are regularly updated to keep pace with the latest technology and security practices.

11. **Integrate security into IoT acquisition.** Incentivize departments and agencies in the procurement process to prioritize secure, interoperable, and scalable IoT solutions for assets based on voluntary, industry-led, consensus-based, global guidelines.

12. **Include IoT in incident response.** Integrate IoT considerations into incident response planning, including policies for IoT incidents and emergency responses.